PCCW Global and Crypteia Networks cyber security services wins innovation award for using big data analytics, machine learning technology, and global threat intelligence to proactively defend client enterprise networks around the world. Crypteia Networks' CEO, Yiannis Giokas, explains

How to beat the cyber attacks worldwide by identifying threats on a global scale

Yiannis Giokas: As cyber threats become more sophisticated and prevalent, our clients increasingly demand better and more responsive protections. The combination of PCCW Global's network footprint with Crypteia's MOREAL threat monitoring capabilities now delivers the market's most comprehensive cyber security solution.

Today's networked enterprise is at risk

Enterprise infrastructures are more at risk today than ever before, says Yiannis Giokas, CEO and founder of Crypteia Networks, PCCW Global's cyber security subsidiary based in Athens, Greece. But by how much? Do corporate names like Sony Pictures, Target Stores and Deutsche Telekom ring a bell?

"Every year companies are spending more than $67 billion on security solutions and services," he says, quoting figures from the industry analyst firm Gartner Group. "But cyber attacks are still leading to more than $4 trillion of damage."

This is happening due to four main reasons, says Giokas, who set up Crypteia Networks in 2011. The company won a Global Telecoms Business Innovation Award — along with PCCW Global — in May 2015 for its use of big data analytics, machine learning technology, and global threat intelligence to proactively protect enterprise networks around the world. According to Giokas:

- Optimising the security infrastructure and maintaining that posture is nearly impossible to achieve;
- A unified process to exchange zero-day security vulnerabilities does not exist (yet);
- Threat actors have increasingly malicious motives as to achieve destructive and financial impact; and
- A digital society does not pay as adequate attention today to safeguarding its online activities (also called the "weak link").

Giokas explains that while publicly visible attacks can have embarrassing and reputational impact on an organisation, it often translates into significant financial and liability impact. The Target Stores attack, for example, cost the company more than $162 million, not to mention the jobs of many senior company officials.

According to PricewaterhouseCoopers, the number of reported security incidents increased by 48% in 2014 over the previous year, to 42.8 million or the equivalent of 120,000 attacks a day.

Addressing the threat

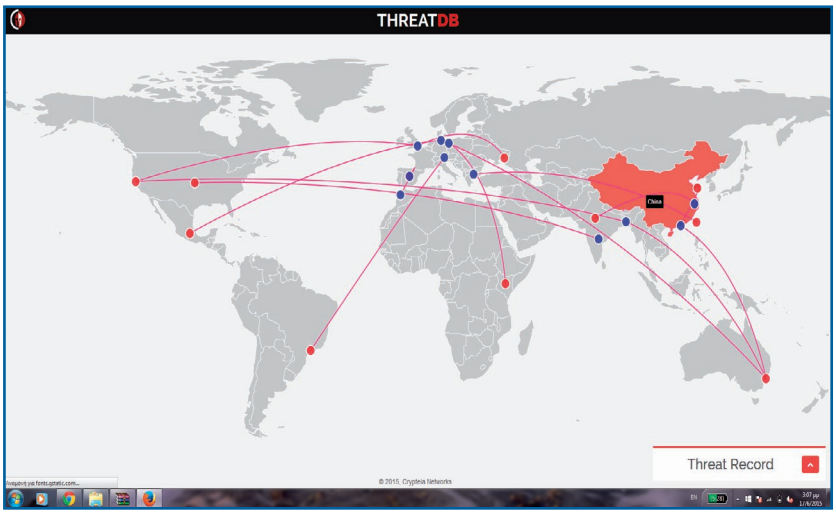
So where are the threats coming from? "Threats are classified based on the goal of the attack," says Giokas. "Financial-driven attacks typically are made by cyber thieves; service disruption attacks (that can impact web site performance and other online activities) usually are initiated by hacktivists or competitors; and data leakage attacks can derive from multiple sources, such as cyber criminals, nation states, competitors, and so on."

The GTB Innovation Awards nomination recognises the collaboration between the global communications service provider PCCW Global and cyber security services experts Crypteia Networks — a wholly-owned subsidiary of PCCW Global — to deliver self-learning network security and threat identification on a global scale.

The solution – MOREAL

According to the nomination, PCCW Global enterprises around the world can now protect their organisations from malicious attacks by adopting Crypteia's MOREAL threat management service, allowing them to benefit from having access to a truly global threat intelligence monitor and database. The solution combines real-time network analytics and machine learning with enterprise networking expertise to deliver a unique approach to network security.

MOREAL is a cloud-based network security solution for enterprises that is able to proactively predict, discover and identify network security threats by mining the data activity logs produced by connected network elements, such as firewalls, routers, intrusion detection tools and other security devices, in order to evaluate patterns and behaviours consistent with a potential cyber attack.



Crypteia's MOREAL is able to evaluate patterns and behaviours from not just a single enterprise but from the entire network, and can parse the data and threat activities by region, industry, and other segments

Most security applications and services in the market rely on recognising known vulnerabilities and exploits rather than identifying new or constantly changing threats. "This is why MOREAL has become an extremely powerful tool for enterprises, as it leverages existing data in the network to provide usable information to the enterprise via a simple dashboard, whilst continually evolving to combat emerging threats," says Giokas.

The latest version of MOREAL was launched in May 2015, and became available on a global scale via the PCCW Global communications network. The operator's network extends to 3,000 cities and 140 countries around the world, enabling MOREAL to capture and mine data traffic patterns worldwide.

In this way, the solution is able to evaluate patterns and behaviours from not just a single enterprise but from the entire network, and can parse the data and threat activities by region, industry, and other segments, delivering to clients actionable information more relevant to their own ecosystem. As a result, PCCW Global and Crypteia Networks are using their combined strengths to deliver a network security solution which for the first time is capable of evolving as rapidly as the network threats it is designed to combat.

Giokas adds: "Threats are becoming more and more sophisticated, so within this scope, PCCW Global, through the Crypteia Networks acquisition, wanted to leverage the data science capabilities that we are offering within the cyber security domain. The MOREAL platform that we have developed is self-defining what a threat is and is not based on its data analysis and algorithmic capabilities."

Crypteia Networks was founded in order to redefine the way security operation centres function. "We were a hungry cybersecurity start-up and our core team had a strong security and software development background that led to the creation of the MOREAL threat intelligence platform," he says. Giokas explains the role of real-time network analytics and machine learning in this approach. "In the security domain, the ability to have a holistic view of your network and the threats that you are exposed to — based on the importance of your assets — is very important."

He continues: "Within this scope, real-time analytics are crucial for today's environments. Furthermore, it is true that people in their day-to-day life are utilising connected systems that are potentially exposed to exploitable threats. Consequently, it is critical to have the ability to understand, monitor and collect user behaviour in order to accurately position the infrastructure in an optimal secure posture. But of course, we shouldn't re-invent the wheel each time a new user or a new deployment is made, and that is where machine learning is coming into the picture."

The algorithms can identify similarities and predictive behaviours. Feedback helps to identify behaviour which is seen to be threatening. "MOREAL can do this lightning fast and even prevent them before they happen," says Giokas.

Security management moves to the cloud

Crypteia Networks ensures that a cloud-based network security management solution remains secure by leveraging the fundamental benefits of the cloud itself. "Cloud infrastructure is operated by a large number of engineers with different backgrounds — people in areas such as development operations, IT, network, security and so on, with vast experience in environments such as PCCW Global, Amazon, SoftLayer, Microsoft, Google and others. They outnumber and have more experience than most corporations' IT and security teams," Giokas says.

"Additionally, cloud computing is eliminating a number of limitations that on-premise solutions have, such as power outages, CPU/RAM/storage faults, and of course CAPEX costs."

He adds: "The same security measures that someone would take in an on-premise solution are today used in cloud environments. Thus, a cloud approach today should be considered an extension of the LAN and not a different domain with different rules."

Giokas explains how quickly the solution can adapt to new or constantly changing threats. "The MOREAL threat intelligence platform is aggregating threat-related knowledge constantly and in real-time, combining it with the outcome of the analysis we do in PCCW Global's IP network, as well as our customers' networks, so our visibility in the evolving threat landscape is constantly growing".

"On top of that, MOREAL's machine-learning capabilities enable it to self-define whether legitimate lookalike behaviours are actually legit or not — and this constant intelligence is the key differentiator that makes the PCCW Global solution fast and accurate."

But there is something else: "Our security operation centres and our security research teams are constantly adding knowledge into our threat database, so our adaptability to the evolution of threats is virtually in real-time," he says.

MOREAL, as a cloud-based solution, is available in all geographic sectors where PCCW Global is offering its services. Crypteia Networks, as part of PCCW Global, is offering its services both to PCCW Global customers and to others, as well via its channel partners. ■

www.pccwglobal.com

See a demo of MOREAL online at www.crypteianetworks.com